An tÚdarás Pinsean
The Pensions Authority

# Digital Operational Resilience Act (DORA) Regulation

## What is DORA?

DORA is an EU Regulation that aims to strengthen digital operational resilience in the financial sector by introducing harmonised requirements for financial entities on the use of information and communication technology (ICT) services.

DORA aims to ensure that ICT risks are managed by financial entities, including pension schemes.

In preparation for DORA, trustees will need to identify any scheme activity that is supported by ICT systems and services, paying particular attention to critical or important functions. Trustees will also need to identify the third parties providing those ICT services and ensure that relevant outsourcing contracts contain provisions that facilitate compliance with the new requirements.

## When does DORA come into force?

The regulation will apply from 17 January 2025.

Trustees will bear ultimate responsibility for ensuring their scheme's compliance with the requirements, irrespective of any outsourcing arrangements in place.

## Schemes subject to DORA

The manner in which the DORA requirements apply to a scheme will depend on the size of the scheme's active and deferred membership.

- Schemes with 100 or more active and deferred members are subject to all DORA requirements.
- Schemes with 16-99 active and deferred members are subject to most of the DORA requirements. However, a simplified version of the ICT risk management framework applies for these schemes, and they are exempt from performing advanced testing of ICT systems and from having to adopt a strategy on ICT third-party risk.
- Schemes with 15 or less active and deferred members are not subject to DORA.

## Overview of DORA requirements

The main requirements for trustees will include:

- Documenting and maintaining a comprehensive ICT risk management framework to include ICT business continuity plans and other policies and controls, as part of the overall risk management system.
- Identifying all sources of ICT risk and cyber threats on a continuous basis together with ongoing monitoring of the security and functioning of ICT systems relied on.
- Effective management of ICT third-party risks ensuring that key contractual provisions are in place with service providers as set out in article 30 of DORA.
- Maintaining a register of information on all contractual arrangements on the use of ICT services provided by third-party providers.
- Managing and reporting major ICT related incidents to the Pensions Authority and keeping a record of significant cyber threats.
- Testing ICT systems supporting critical or important functions at least yearly.

## Links to legislation

The full range of DORA requirements is set out in the DORA regulation and the accompanying technical standards which provide templates and further details about the requirements. Further information is available at the links below:

ICT and third-party risk management and incident classification - European Union (europa.eu)

Second batch of policy products under DORA (europa.eu)